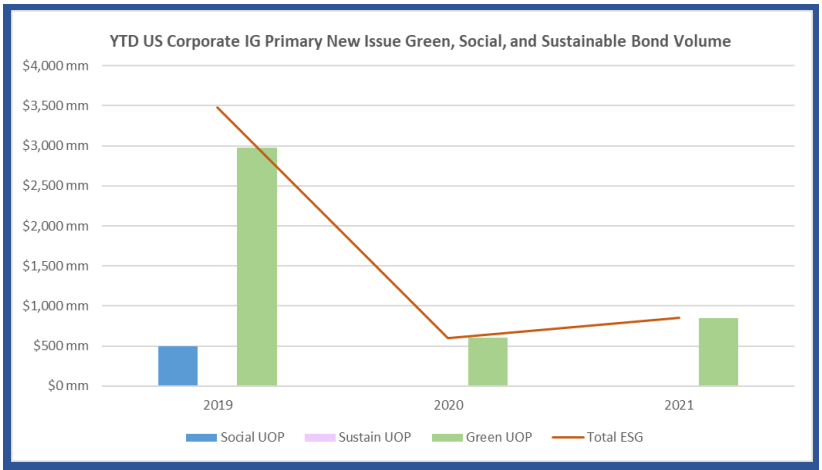
January 2021

One of the key themes to emerge from the new Biden Presidency is federal re-engagement on the environment, more specifically, climate. This appears to be a 180-degree shift from the Trump administration's approach. Announcements have been made cancelling the Keystone XL pipeline. President Biden also said that the US will rejoin the Paris Climate Agreement. Finally, Janet Yellen has made comments regarding how the Fed will consider a new climate initiative.



2021 has brought forth two green bond transactions from Duke Realty and Southern Company, totaling to $850mm YTD IG ESG issuance.

However, the focus of this report is on a different type of environment: our digital one.

An Expanding Attack Surface

In the 1980's, only about 10% of the economy was reliant on the use of silicon chips. Today, it is more than 80%. COVID-19 has continued accelerating this as global average customer digital interaction increased from 36% in December 2019 to 58% in July 2020. Simultaneously, the government and telcos are working hard to close the rural broadband gap and bring more Americans online with access to digital marketplaces and services.

As we continue to leverage digital environments in lieu of physical ones, we also continue to expand our attack surface to threat actors (foreign nation states and others). Last year's SolarWinds breach was one of the most recent and was very expansive in its reach. If you have not had the opportunity to review our latest webinar "Geostrategic Surprises for 2021 & Cybersecurity" featuring our macro strategist and generals from our Geopolitical Intelligence Group, we would highly recommend that you view the webinar when you can. It includes some unique insight from US Marine Corps Lt. General Vince Stewart, who held senior leadership roles at both the Defense Intelligence Agency and US Cyber Command.

Financially, the impacts of breaches cannot be ignored. Last year the FBI's IC3 reported $3.5bn in internet fraud, including $1.7bn in total losses related to business email compromise. While the government, healthcare, utility, and financial sectors have been traditional targets for threat actors, other industries like shipping/transport and higher education are now finding themselves in the crosshairs. Threat actors are also becoming more sophisticated in both methodology and targeting. For instance, the FBI reported a 40% yearly increase in total losses associated with Tech Support fraud (i.e., threat actors posing as service representatives).

Policy Response

So far the Biden administration has already announced that as part of its proposed $1.9 trillion COVID Rescue Plan, $9bn would be allocated to cyber modernization across 18 federal agencies, $200mm would be spent to acquire talent, and $600mm+ would be earmarked to enhance cybersecurity throughout federal and civilian networks—substantially boosting the resources of the US Cybersecurity Infrastructure Agency. The administration will probably also look to incorporate recommendations made by the Cybersecurity Solarium Commission's report which describes the current status quo of cyberspace as "unacceptable" and calls for a layered approach that shapes behavior, denies benefits, and imposes costs.

Such actions by the Biden administration could add to an already expected $60bn in global cybersecurity spending. Any policy changes on national cyber security strategy will be of material importance to the 16 critical infrastructure sectors whose assets and networks are considered vital to the United States. Companies considered part of critical

infrastructure may have to build out capabilities or workforces that allow them to adapt to a new national cyber security strategy. This could include personnel, hardware, consultation, and training.

Simultaneously there is now discussion coming from the Senate to reexamine national breach legislation. Currently private companies must disclose a breach/hack to the SEC only if it meets a threshold for materiality. This may soon change in the wake of SolarWinds as the Senate looks to review and possibly lower that threshold. Despite bipartisan support on issues of cybersecurity, it remains to be determined if the proposal will gain traction. However, if it were to come to fruition, it would have significant impact on smaller companies which would have to invest in increased network security to avoid breaches. It could also impact IPOs, as investors will want to know more about their investment's cybersecurity practices and outcomes. Cyber Self-Regulatory Association is on the table too!

Looking Ahead…Opportunities for Cyber Financing

With a renewed focus by the Biden administration on cybersecurity and an increasing focus by ESG investors, there is a real opportunity for organizations to leverage capital markets and sustainable financing to help fund expenses needed to help secure networks and personal/public data. Last year was a banner year for sustainability bonds, which incorporated a combination of the ICMA's green and social bond principles. Moving forward, issuers should seriously consider incorporating cybersecurity project financing into their sustainability bond frameworks. Challenges related to reporting will remain the biggest hurdle, as issuers are hesitant to disclose information related to cybersecurity that threat actors could exploit. A possible work around could be thematic classification, for instance "Cybersecurity Hardware", and aggregating related expenses without exposing details.

Like investments being made to keep our physical environment safe and clean (EV vehicles, solar, wind, water conservation etc.), we must also look to invest and keep our digital frontier secure.

Further Resources

President Biden's America Rescue Plan: https://buildbackbetter.gov/wp-content/uploads/2021/01/COVID_Relief-Package-Fact-Sheet.pdf

McKinsey Report: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

FBI IC3 Report: https://pdf.ic3.gov/2019_IC3Report.pdf

Impact of Computing on World Economy: https://www.cse.unr.edu/~fredh/papers/conf/074-iocotweapp/paper.pdf

Cyber Security Solarium Commission Report: https://www.solarium.gov/report

CISA: https://www.cisa.gov/critical-infrastructure-sectors

Washington Post: https://www.washingtonpost.com/politics/2021/01/15/cybersecurity-202-sen-mark-warner-plans-breach-notification-debate-wake-solarwinds-hack/